Real-Time Visual Analytics for Event Data Streams

Fabian Fischer, Florian Mansmann, Daniel A. Keim

Fabian Fischer  |  Data Analysis and Visualization Group  |  University of Konstanz
Interactive Visualization

is a way to tightly combine human factors and data analysis.

Visual Analytics
Use Case for Event Streams

Analyzing System Log Events
(event stream of server log messages)
Framework Architecture
Real-Time Visual Analytics for Event Data Streams

Data Streams → Event Service

Event Service → Message Broker

Message Broker → Event Analyzer(s)

Event Analyzer(s) → Data Storage

Data Storage → Event Visualizer

Event Visualizer subscribes to topics.

Message Broker subscribes to queues.

Event Analyzer(s) inputs raw messages and outputs analyzed events.

Data Storage connects to data storage.

Normalization, Fingerprint, Rules, Scoring, Aggregation.
Relaxed Event Timeline Visualization

Focus on Temporal Aspect of Data Streams (Monitoring & Exploration)

S1: A K
S2: B E J
S3: C D F G H I

color mapped to priority

selected scale: one hour (h)

$h_{now} - 1$

$h_{now}$

now
Demo/Video
Main Contributions

• Generic processing and analysis architecture for event data streams to support real-time visual analytics applications.

• A system for pluggable visualizations for real-time and historical event data.

• Dynamic timeline visualization to directly interact with multiple streams to visualize highly co-occurring events.
Future Work

• Controlled system evaluation.
• Integration of advanced algorithms for burst and anomaly detection.
• Integration of more visualizations based on the learned design principles.

• Use the Event Visualizer for other datasets.
  – Feb 2012 – Successful participation in the Honeynet Forensic Challenge 2011/10 [1].

Thank you very much for your attention!

Questions?

For more information about this work or about visual analytics please contact

**Fabian Fischer**
Tel. +49 7531 88-2780
Fabian.Fischer@uni-konstanz.de

http://ff.cx/
References I

Illuminating the Path: The Research and Development Agenda for Visual Analytics.
*IEEE Computer Society, 2005.*

Visualization of Time-Oriented Data.
References II


**Visual Analysis of Dynamic Data Streams.**
*Information Visualization, 8(3):212-229, 2009.*


**Visual Pattern Discovery in Timed Event Data.**
*In Proceedings of Conference on Visualization and Data Analysis, 2011.*